IMPLEMENTASI KRIPTOGRAFI BLOWFISH PADA SEBUAH INFORMASI DALAM BENTUK QR CODE

[1]Fahmi Luthfillah (11 1065 1161)
[2]Ari Eko Wardoyo S.T, M.Kom, [3]Yeni Dwi Rahayu S.St, M.Kom
Program Studi Teknik Informatika Fakultas Teknik
Universitas Muhammadiyah Jember
Email: *fahmi.luthfillah@gmail.com*

ABSTRAK

Makalah ini memaparkan bagaimana mengamankan dokumen dengan menggunakan Algotirma Blowfish yang dipadukan dengan *QR Code* dan *base64* untuk mencegah pemalsuan dokumen. Pada saat ini teknologi informasi berkembang sangat pesat, seiring dengan perkembangan teknologi berkembang pula bahasa pemrograman dan teknologi pengamanan dokumen. Dokumen merupakan hal yang sangat penting bagi setiap orang, negara, instansi maupun perusahaan. Oleh karena itu diperlukan suatu teknologi yang berguna untuk menjaga keamanan dan kerahasiaan dokumen. Kriptografi merupakan ilmu yang mempelajari bagaimana supaya pesan atau dokumen kita aman agar tidak mudah dipalsukan oleh pihak yang tidak berhak. Dalam pembuatan aplikasi keamanan dokumen ini, penulis menggunakan algoritma *Blowfish* yang dikombinasikan dengan *base64* dan *QR Code* (*Quick Response Code*). Penulis menggunakan *Java Mobile Android* sebagai bahasa pemrograman dan Eclipse Luna sebagai pembuatan aplikasi. Metode penelitian yang penulis gunakan terdiri dari studi pustaka dan literatur. Hasil akhir berupa aplikasi berbasis *Mobile Android* yang bisa di install dari versi android 2.2 sampai 5.1. Aplikasi dapat menghasilkan pengamanan yang sangat baik dalam mengamankan dokumen.

Kata kunci : Kriptografi, Dokumen, Teknologi, Informasi, *QR Code* (*Quick Response Code*), enkripsi, base64, Android, Java Mobile, Eclipse

1. PENDAHULUAN

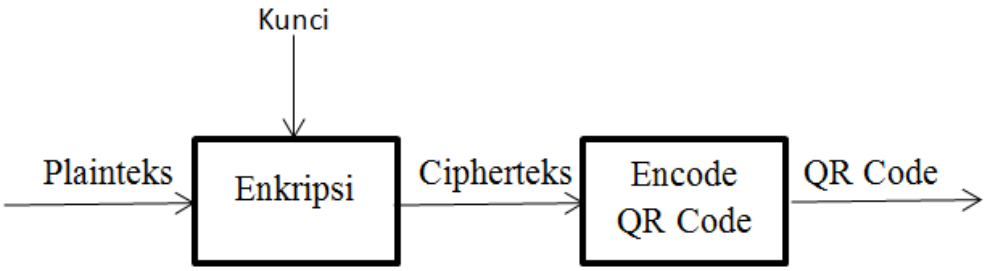
Dokumen merupakan salah satu data yang sangat penting karena merupakan sumber informasi yang diperlukan oleh suatu instansi, organisasi, atau Negara. Selain sumber informasi dokumen dipakai sebagai bukti keterangan. Ada macam-macam bentuk dokumen, bisa berbentuk surat, gambar ataupun rekaman suara. Seiring perkembangan teknologi dan informasi, manipulasi terhadap gambar, teks, atau berkas-berkas termasuk dokumen atau sertifikat hasil test, sangat mudah dilakukan. Sehingga dapat memberikan celah untuk melaksanakan praktik pemalsuan dokumen. Untuk mengantisipasi terjadinya pemalsuan, maka dilakukan pengamanan dengan cara menyisipkan suatu objek pengenal seperti pemilik, ID, tanggal berakhirnya dan nilai/score dokumen sertifikat yang digunakan untuk mencocokkan konten yang tertulis pada dokumen, yang kemudian akan disisipkan dan diproses menjadi sebuah kode yang dapat diidentifikasi dan dicocokkan. *QR Code* (*Quick Response Code*) merupakan teknik yang mengubah data tertulis menjadi kode-kode 2-dimensi yang tercetak kedalam suatu media yang lebih ringkas.(Anita Rahmawati, Arif Rahman. 2011). Dengan *QR Code* informasi keaslian sertifikat tersebut dibuat menjadi lebih sederhana atau *simple* tanpa mengetikkan informasi kode validasi pada dokumen tersebut. Praktik pemalsuan masih dapat dilakukan terhadap konten *QR Code*. Untuk itu perlu dilakukan proses enkripsi konten, sebelum diubah ke *QR Code*. Tujuan enkripsi adalah agar konten yang diubah ke dalam *QR Code* tidak dapat diidentifikasi secara langsung format dan isinya oleh orang lain. Untuk mengatasi masalah kemananan keaslian dokumen maka digunakan Algoritma Blowfish.

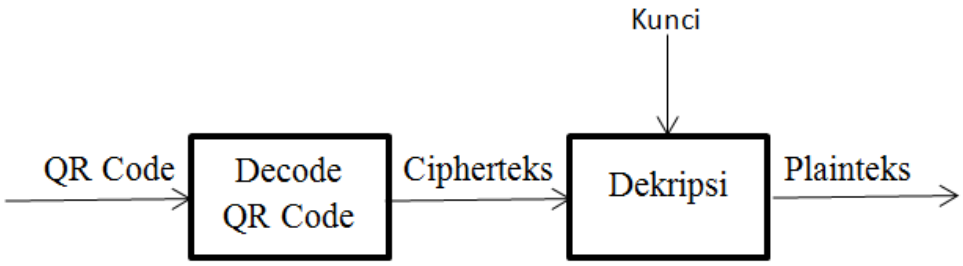
2. METODELOGI PENELITIAN

2.1 Perancangan Sistem

Tujuan dari perancangan sistem adalah untuk memenuhi kebutuhan pengguna mengenai gambaran yang jelas tentang perancangan sistem yang akan dibuat serta diimplementasikan. Untuk mulai membangun suatu aplikasi kriptografi, maka penulis terlebih dahulu merencanakan

alur kerja berdasarkan kebutuhan pengguna yang akan menggunakan aplikasi ini.





Gambar 2.1 Diagram Blok Enkripsi

Gambar 2.2 Diagram Blok Dekripsi

2.2 Metode Pengujian

Ada dua metode pengujian yang akan dilakukan penulis sebagai berikut :

1. Setelah aplikasi selesai dibangun, pengujian akan dilakukan dengan menggunakan beberapa *smartphone* dengan lebar layar yang berbeda-beda untuk menentukan kualitas gambar *QR Code* yang dihasilkan dari aplikasi. Berikut beberapa *smartphone* dengan layar berbeda yang akan diuji dapat dilihat pada tabel 2.1 :

Tabel 2.1 Nama dan Spesifikasi Smartphone

Nama *Smartphone*	Spesifikasi
Xiaomi Redmi 1s	Type : IPS LCD capacitive touchscreen, 16M colors Size : 4.7 inches (~64.4% screen-to-body ratio) Resolution : 720 x 1280 pixels (~312 ppi pixel density) Multitouch : Yes Protection : AGC Dragontrail glass OS : Android OS, v4.3 (Jelly Bean) / MIUI 5.0 Chipset : Qualcomm MSM8228 Snapdragon 400 CPU : Quad-core 1.6 GHz Cortex-A7 GPU : Adreno 305
Samsung Grand Galaxy Prime	Type TFT capacitive touchscreen, 16M colors Size 5.0 inches (~66.0% screen-to-body ratio) Resolution 540 x 960 pixels (~220 ppi pixel density) Multitouch Yes OS Android OS, v4.4.4 (KitKat) Chipset Qualcomm MSM8916 Snapdragon 410 CPU Quad-core 1.2 GHz Cortex-A53 GPU Adreno 306

2. Setelah aplikasi selesai dibangun, metode pengujian kedua akan dilakukan pada dokumen yang sudah diberikan *QR-Code* dengan menggunakan aplikasi yang telah dibuat.

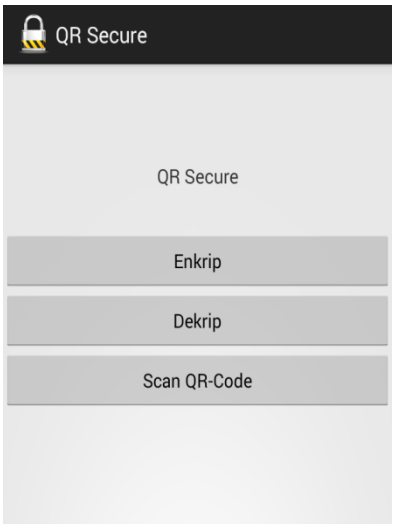
3. HASIL DAN PEMBAHASAN

3.1 Implementasi

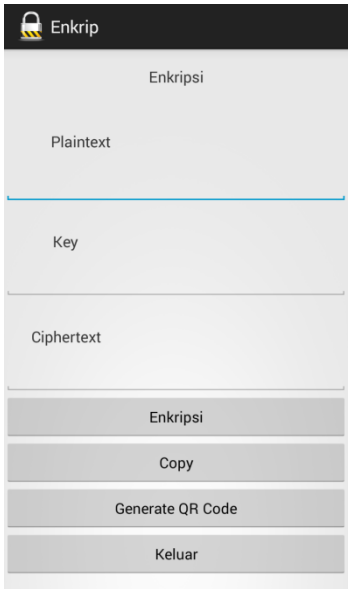
Setelah melakukan analisis sistem, tahap berikutnya adalah implementasi, pada tahap ini sistem dibangun dengan segala kebutuhan sistem.

3.2 Tampilan Aplikasi

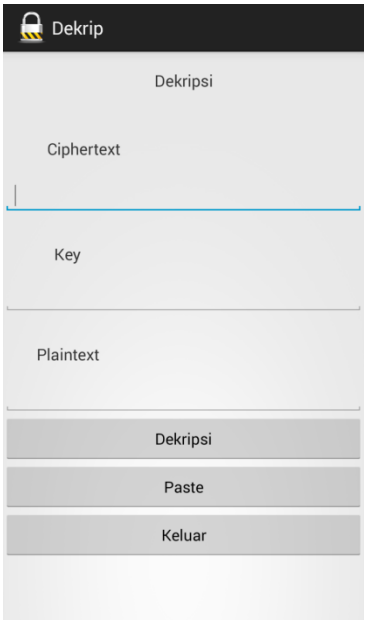
Berikut tampilan aplikasi ketika dijalankan menggunakan *smartphone*



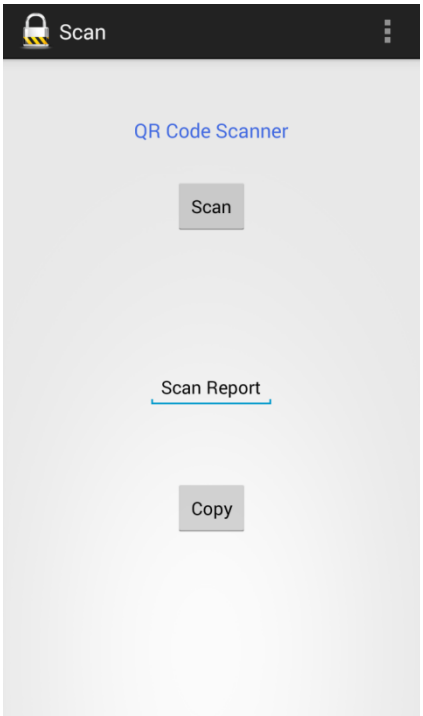
Gambar 3.1 Tampilan Menu Utama



Gambar 3.2 Tampilan Menu Enkrip



Gambar 3.3 Tampilan Menu Dekrip



Gambar 3.4 Tampilan Menu Scan

3.3 Pengujian Aplikasi Pada Dokumen

Berikut langkah-langkah pengujian aplikasi pada dokumen.

Peratama tentukan *plaiantext* pada dokumen yang akan di enkripsi. Dokumen yang akan dibuat sebagai contoh merupakan judul sidang tugas akhir penulis. *Plaintext* sebagai berikut :

Nama : Fahmi Luthfillah

NIM : 1110651161

Jurusan : Informatika

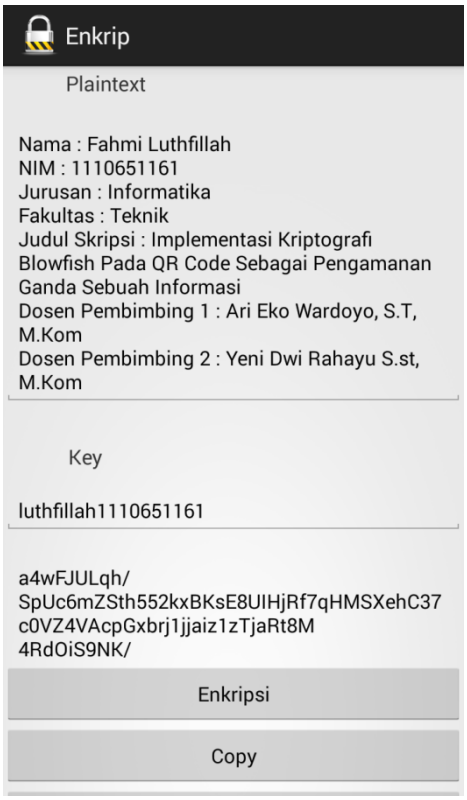
Fakultas : Teknik

Judul Skripsi : Impelemntasi Kriptografi Blowfish Pada QR Code Sebagai Pengamanan Ganda Sebuah Informasi

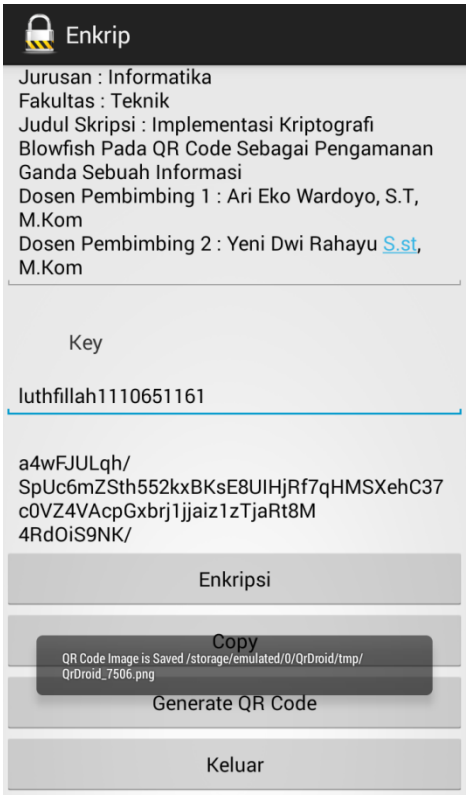
Dosen Pembimbing 1 : Ari Eko Wardoyo, S.T, M.Kom

Dosen Pembimbing 2 : Yeni Dwi Rahayau S.st, M.Kom

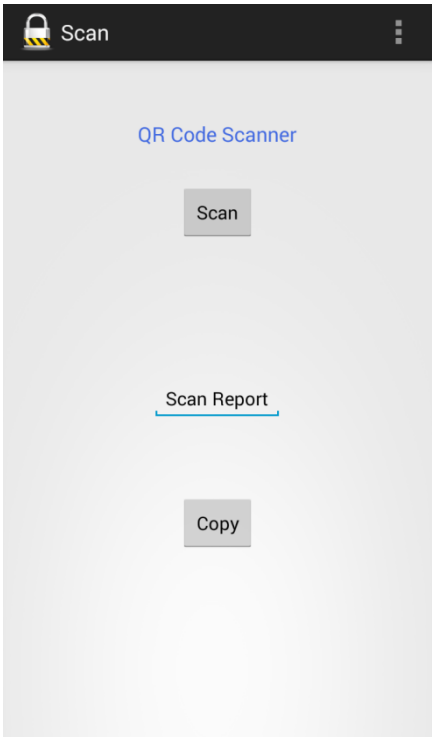
Kemudian kunci yang akan digunakan luthfillah1110651161



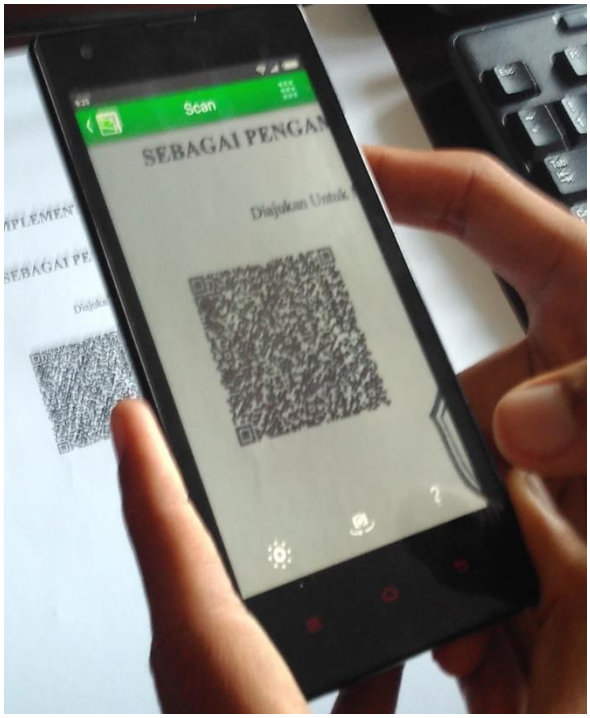
3.7 Proses Enkrip



3.6 Proses Generate QR Code

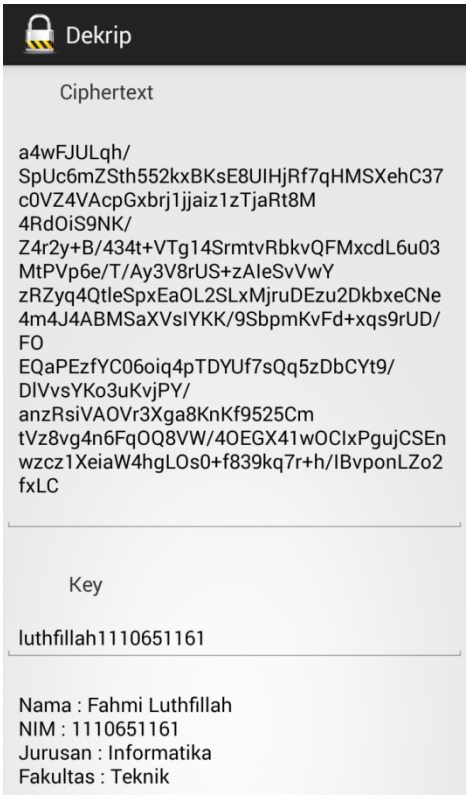


3.7 Proses Scan Tahap 1



Gambar 3.8 Proses Scan tahap 2

Gambar 3.9 Hasil Scan



Gambar 3.10 Proses Dekrip

3.4 Pengujian Aplikasi Pada Layar Smartphone

Setelah melakukan pengujian pada dua *smartphone* dengan layar yang berbeda penulis ternyata tidak menemukan perubahan. Dimensi layar yang dgunakan 4.7'' dan 5.0''. Ukuran *pixel* yang dihasilkan terlihat sama yang berukuran 576px x 576px. Dibawah ini contoh QR-Code dari dua layar *smartphone* yang berbeda :

Gambar 3.11 QR-Code Pada Layar 5.0''

Gambar 3.12 QR-Code Pada Layar 4.5’’

4. KESIMPULAN DAN SARAN

4.1 Kesimpulan

Aplikasi kriptografi ini merupakan kriptografi yang mengadopsi dari metode *blowfish* yang bekerja dengan 16 iterasi untuk mendapatkan hasil berupa *ciphertext* yang setelah itu dikombinasikan dengan base64 sehingga lebih mempersulit untuk pihak yang tidak bertanggung jawab untuk memecahkan *ciphertext*.

Dari hasil Implementasi dan Pengujian dapat disimpulkan sebagai berikut:

1. Algoritma *Blowfish* dapat diimplementasikan pada QR-Code.
2. Algoritma *Blowfish* dapat di implementasikan dengan base64.

4.2 Saran

Aplikasi kriptografi ini merupakan aplikasi mobile android yang menggunakan tambahan library untuk menghasilkan QR-Code. Algoritma *Blowfish* yang dipadukan dengan base64 sangat baik namun masih memiliki kekurangan karena ciri dari base64 yang sudah diketahui public. Diharapkan akan ada aplikasi kriptografi yang lebih baik untuk pengembangan selanjutnya.

DAFTAR PUSTAKA

Fahmi, H., and Faidah, H. 2010. *Aplikasi Kritpografi Modern untuk Pengiriman Data Teramankan*. MH Thamrin 8. Jakarta.

Franindo, A. 2007. *Chiper Blok dengan Algoritma Operasi XOR antar Pecahan Blok. Jurnal Teknik Informatika ITB*. Bandung.

Fridh Zurriyadi Ridwan, Hariyo Santoso, dan Wiseto P. Agung. 2010. *Mengamankan Single Identity Number (SIN) Menggunakan QR Code dan Sidik Jari*. PT Telekomunikasi Indonesia.

Guritman, Sugi., Rachmaniah, Meuthia., Merdiana, Dian. 2003. *Algoritma Blowfish untuk Penyandian Pesan*. Staf Jurusan Ilmu Komputer Fakultas Matematika dan Ilmu Pengetahuan Alam dan Mahasiswa Jurusan Ilmu Komputer Fakultas Matematika dan Ilmu Pengetahuan Alam.

Khairunnisa, Desy Eka. 2012. Pembuatan Aplikasi Enkripsi Informasi Surat Keputusan Menggunakan Metode Blowfish Studi Kasus PT. Asuransi Kredit Indonesia (ASKRINDO). UIN Syarif Hidayatullah Jakarta.

Pasca, Nugraha, M., Munir, Rinaldi. 2011. *Pengembangan Aplikasi QR Code Generator dan QR Code Reader dari Data Berbentuk Image*. Institut Teknologi Bandung Jl. Ganesha 10 Bandung 40132.

Rahmawati, Anita., Rahman, Arif. 2011. *Sistem Pengamanan Keaslian Ijasah Menggunakan QR-Code dan Algoritma Base64.* Program Studi Sistem Informasi, Universitas Ahmad Dahlan

Sarno, R. dan Iffano, I. 2009. *Sistem Manajemen Keamanan Informasi. Surabaya: ITS Press.*.

Satria, Eko. 2009. *Studi Algoritma Rijndael dalam Sistem Keamanan Data.* Universitas Sumatra Utara.

Schneier, Bruce, 1996, Applied Cryptography, Second Edition, John Wiley & Son, New York.

Sitinjak, Suriski., Fauziah, Yuli., Juwairiah. 2010. *Aplikasi Kriptografi File Menggunakan Algoritma Blowfish*. Jurusan Teknik Informatika UPN Veteran Yogyakarta.

Syafari, Anjar, 2007. Sekilas Tentang Enkripsi Blowfish, http://www.ilmukomputer.com, diakses sejak tanggal 08 Mei 2015.

Tresnani, Dini Lestari., 2012. *Implementasi Sistem Absensi Menggunakan QR Code Pada Smartphone Berbasis Android.* Teknik Informatika. Institut Teknologi Bandung.